APPLICATION FOR UNITED STATES LETTERS PATENT

by

STEVEN G. SMITH,
GARY J. DENNIS,
RALPH J. MILLS,
ROLAND T. MORTON, JR.,
CURT KALOUSTIAN,
JEFFREY A. SYLVESTER, AND
MITCHELL E. DAVIS

for

TECHNICIAN WIRELINE AND WIRELESS INTRANET ACCESS VIA SYSTEMS INTERFACE TO LEGACY SYSTEMS

SHAW PITTMAN
1650 Tysons Boulevard
McLean, VA 22102
(703) 770-7900

Attorney Docket No.: BS00-354
1138045/1138058

TECHNICIAN WIRELINE AND WIRELESS INTRANET ACCESS VIA SYSTEMS INTERFACE TO LEGACY SYSTEMS

FIELD OF THE INVENTION

[0001] The present invention relates generally to the field of telecommunications dispatching and, more particularly, to methods and apparatus for providing mobile personnel access to a company shared network.

BACKGROUND OF THE INVENTION

[0002] Telecommunications technicians, such as so-called "Installation and Maintenance" (I&M) technicians, may visit customer sites to install new equipment, set up new services, or to service existing equipment or services. Frequently an I&M technician needs to gather local or district-specific information to complete a "job order" or task. For example, an I&M technician may need to know cross-box locations, pricing information, service information, cable records, plat information, or other information needed to carry out his or her assignment.

[0003] For many telephone companies, including Regional Bell Operating Companies (RBOCs), such local information is generally not stored on centralized legacy systems. Accordingly, although I&M technicians can presently access information stored on these central legacy systems using

portable laptops and custom software, they are unable to remotely access the local information using their portable laptops.

[0004] According to the conventional approach to this problem, an I&M technician seeking local information must make one or more telephone calls to local offices of his or her employer. Several calls may be required. The I&M technician may be put on hold as the call attendant collects the information or tends to other business. The time the I&M technician must spend in collecting local information reduces his or her job efficiency and may increase costs to customers. Furthermore, miscommunications between individuals may cause incorrect information to be transferred. For example, the data retrieved by the call attendant may not be accurately interpreted by the call attendant who has a lower level of technical expertise then the I&M technician. These are significant drawbacks to the current approach.

SUMMARY OF THE INVENTION

[0005] The present invention is generally directed to a system and method for permitting a user to access local information stored on a company shared network or an intranet. In the present invention, a user logs a computer into a systems interface which permits access to back-end legacy systems. The computer accesses the systems interface over a wireline or a wireless communications network. Preferably, the systems interface is located at or associated with at least one network address.

[0006] Preferably, the systems interface includes a first server with middleware for managing the protocol interface, and the first server is located at or associated with a first network address. Preferably, the systems interface includes a second server for receiving requests and generating legacy transactions. When the user is logged in, a client application for the systems interface is running on the computer.

[0007] Next, the user launches a shared network software application, preferably a browser. The user may or may not minimize the client application, but the user remains logged in. As the browser launches and seeks out an intranet site at a separate network address, the systems interface receives a message from the computer or otherwise detects that the computer is seeking access to the intranet. The user can manually enter, or through a previous bookmarking procedure, provide, the network address of the desired "target" web page. When this network address is received, access to the Intranet begins.

[0008] In response to detecting that the computer seeks access to the intranet, the systems interface determines whether intranet access is to be granted. If access is granted, the systems interface routes communications from the computer to the separate network address. The middleware passes the session (the requested data transaction) on to the network address that is input with TechNet, and the network address of the TechNet server is transmitted. Other network addresses sent by the browser are passed by the middleware.

Preferably, the first server routes the computer from the first network address to the separate network address. The user is then logged into an operations support systems (OSS), and connectivity to the OSS is maintained while access to Intranet is being accomplished.

[0009] The advantages of the present invention are numerous. The invention permits a technician to remotely access local or district-specific information without making a series of telephone calls to local offices. The initial log-on to the systems interface provides a measure of security, yet a separate log-on to the intranet is not required. When accessing the intranet, the computer remains logged on to the systems interface so that a return to the systems interface, for example, to access the legacy systems, is readily achieved. For example, in addition to overcoming the limitations described above, the present invention makes available information that is otherwise inaccessible to the technician. Furthermore, the technician can also provide direct input to intranet accessed systems, databases, and information repositories.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is a schematic block diagram of a system for allowing user access to an intranet according to one embodiment of the invention.

[0011] FIG. 2 is a schematic block diagram of a system for allowing user access to an intranet according to another embodiment of the invention.

[0012] FIG. 3 is a flow diagram of a method for a user to access an intranet according to one embodiment of the invention.

[0013] FIG. 4 is a flow diagram of a method for allowing a user to access an intranet according to another embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0014] FIG. 1 is a schematic block diagram of an exemplary system for allowing a user, such as a technician, to access an intranet according to one embodiment of the invention. The system of FIG. 1 includes computer 100, communications network 120, systems interface 130, back-end legacy systems 140, and intranet 150.

[0015] Computer 100 is a computer used by a technician or other service person to access information from back-end legacy systems 140. As used herein, "computer" is used in the broadest sense of the term. A "computer" may be a microcomputer, minicomputer, laptop, personal data assistant, cellular phone, two-way pager, processor, or any computerized device capable of transmitting and receiving data over a shared network. Preferably, computer 100 is a ruggedized laptop computer.

[0016] Computer 100 remotely accesses systems interface 130 through communications network 120. Communications network 120 may be any communications network that permits a remote computer to access a remote server. Communications network 120 could be a wireline network, wireless or

cellular network, satellite network, or other network permitting a computer to communicate with a remote server. Preferably, communications network 120 is a Public Switched Telephone Network (PSTN). For example, communications network 120 can be BellSouth Communications Network. Alternatively communications network 120 can be a wireless network, such as the Cingular Wireless Network.

[0017] Systems interface 130 provides a systems interface between remote (and preferably portable) computers 100 seeking data from back-end legacy systems 140. Legacy systems 140 are generally mainframe-type computer systems that maintain data for a company. According to an embodiment, legacy systems 140 may include one or more legacy systems including a loop facility assignment control system; a loop maintenance operations system; a computer system for main frame operations; a mechanized loop testing system; a secure network element contract server; a mechanized time reporting system; and a work activity statistical sampling plan system.

[0018] Intranet 150 is a company shared network that includes local information not generally stored or maintained on legacy systems 140. Generally, intranet 150 includes firewalls or similar protections to prevent tampering or intrusion by unauthorized users. Prior to the present invention, intranet 150 was generally inaccessible to technicians operating a computer 100 logged-in to the systems interface 130 to legacy systems 140. As used herein, "company" is intended to have the broadest meaning, and should be

understood to include a company, corporation, association, partnership, limited liability company, and any other group of persons or entities that may store and share data via a shared intranet. Preferably, intranet 150 is an intranet for a telecommunications entity that stores local or district-specific information not generally stored in centralized back-end legacy systems. According to another embodiment, intranet 150 may be or may include an external computer network, for example, the Internet.

[0019] The general operation of the system of FIG. 1 is as follows. A technician with computer 100 logs onto systems interface 130 over communications network 120. After the log-on, systems interface 130 permits computer 100 to submit requests for information. Systems interface 130 processes these requests, generates legacy transactions, receives information from legacy systems 140, and transmits the information back to computer 100. Systems interface 130 is also adapted to allow a user to access intranet 150. If the user is permitted access to intranet 150, computer 100 is routed from systems interface 130 to intranet 150.

[0020] FIG. 2 is a schematic block diagram of an exemplary preferred system for allowing technicians to access an intranet according to another embodiment of the invention. The system of FIG. 2 includes computer 200, modem 220, communications network 230, one or more protocol servers 240, one or more transaction servers 250, firewall 260, legacy systems 270, and company intranet 280.

[0021] Computer 200 is a remote and preferably portable computer (e.g., a ruggedized laptop or notebook computer) used by a technician. Computer 200 may be any of the devices discussed above for computer 100 (FIG. 1).

[0022] Modem 220 is a modem for coding and decoding data transmitted between computer 200 and communications network 230. Depending on whether communications network 230 is wireline or wireless, modem 220 may be a conventional wireline modem or a so-called "cellular modem" or "wireless modem". Preferably, a wireline modem can transmit at 56.6 kb/s or is a v.90 modem. A wireless modem can preferably transmit at about 2 kb/s.

[0023] Communications network 230 may be a wireline communications network. For example, communications network 230 can be a PSTN, such as the BellSouth Communications Network. Alternatively, or in addition, communications network 230 may be a wireless or cellular communications network. For example, communications network 230 can comprise the Cingular Wireless Network. Generally, modem 220 and communications network 230 can support transmission rates in the range of about 2 to 56 kilobits per second, depending on whether the communications link is wireline or wireless.

[0024] Legacy systems 270 and company intranet 280 are similar to and include any of the variations discussed in connection with legacy systems 140 and intranet 150, respectively, of FIG. 1.

[0025] According to FIG. 2, computer 200 accesses legacy systems 270 and company intranet 280 via a systems interface 210. Systems interface 210 can include protocol servers 240 and transaction servers 250. System interface 210 can be protected by firewall 260. Generally, protocol servers 240 provide a protocol and middleware interface between computer 200 and transaction servers 250. Protocol servers 240 may receive requests for information or other messages from computer 200; route requests or messages to input queues in transaction servers 250; receive responsive information from transaction servers 250; and route responsive information back to computer 200.

[0026] Generally, transaction servers 250 provide an interface to back-end legacy systems 270 so that responsive information can be retrieved. Transaction servers 250 may service requests, generate legacy transactions in response to those requests, and receive responsive information to be forwarded back to protocol servers 240.

[0027] In one specific implementation, protocol servers 240 may be NT servers running NetTech software from Broadbeam Corporation of Princeton, New Jersey. Transaction servers 250 may utilize Unix operating system software running an Informix database management system.

[0028] The preferred systems interface (which can be element 130 of FIG. 1 and element 210 of FIG. 2) is disclosed in the copending, commonly owned, U.S. Pat. App. No. 09/343,815, entitled "Systems and Methods for Utilizing a

Communications Network for Providing Mobile Users Access to Legacy Systems (hereinafter, referred to as "the '815 application"), filed on June 30, 1999, the entirety of which is hereby incorporated by reference. The preferred systems interface is described in the aforementioned application in connection with the so-called "TECHNET" system, which includes protocol servers and TechNet servers corresponding to protocol servers 240 and transaction servers 250, respectively.

[0029] According to an embodiment, the "virtual location" (hereinafter, simply the "location") of systems interface 210 is defined by at least one network address. Preferably, the network address comprises an Internet Protocol (IP) address, which is well-known in the art. At least one network address defines the location of systems interface 210. Preferably, the location of protocol servers 240 is defined by a first network address and the location of transaction servers 250 is defined by a second network address.

[0030] The company intranet 280 has its own network address or addresses. Preferably, the network address defining the company intranet 280 is an IP address. The network address of company intranet 280 is referred to herein as a "separate network address" so as to indicate that company intranet 280 is located at a network address separate from the network address of systems interface 210.

[0031] The general operation of the preferred system of FIG. 2 is now described. A user (e.g., a technician) using computer 200 dials up or otherwise

contacts protocol servers 240 via modem 220 and communications network 230. The user may dial up or otherwise contact protocol servers 240 over a communications network 230 that is a wireline network or that is a wireless network. The technician may log-on to the protocol servers 240 using a user name and other data, such as a password and/or primary host group address. Once the technician has been authenticated, a session (hereinafter, a "TechNet session") is established and computer 200 is connected to a protocol server 240 associated with the first network address.

[0032] Preferably, computer 200 is running application-specific client software for interfacing with the systems interface to legacy systems 270. According to an embodiment, computer 200 is running the TechNet client application disclosed in the '815 application.

[0033] Preferably, upon log-on a primary screen or primary graphical user interface (GUI) is transmitted to computer 200. This is referred to herein as the "TechNet home page." A technician may make selections from the TechNet home page to access data from back-end legacy systems 270. For example, the technician may select "Get A Job" to get his or her next task or job order. The information corresponding to the "Get A Job" request (i.e., a job order for that technician) is provided from legacy systems 270. Other requests for information from legacy systems 270 can be initiated by the technician using the TechNet home page.

[0034] Next, the user may wish to access the company intranet 280. Having logged-on to systems interface 210 (e.g., to establish a TechNet session), the user launches a shared network software application. Preferably, this shared network software application is a browser application. The user may or may not minimize the client application, but the user remains logged-on to systems interface 210 (i.e., the user does not close out or end the client application). As the browser launches and seeks out separate network address corresponding to the intranet site, systems interface 210 receives a message from computer 200 or otherwise detects that computer 200 is seeking access to intranet 280. The user may manually supply the separate network address. Alternatively, the separate network address may be previously stored on computer 200. For example, the separate network address can be set as the default home page for the browser or otherwise bookmarked.

[0035] In response to detecting that computer 200 seeks access to intranet 280, systems interface 210 determines whether intranet access is to be granted. For example, transaction servers 250 may confirm that the technician is a valid user who is properly logged-in to a TechNet session. Transaction servers 250 may compare the technician's user ID to a list of authorized (or prohibited) technician intranet users to determine if access to intranet 280 should be granted (or denied).

[0036] If access is granted, the systems interface 210 routes computer 200 to the separate network address corresponding to intranet 280. The middleware

passes the session (the requested data transaction) on the network address that is input with TechNet, and the network address of the TechNet server is transmitted. Other network addresses sent by the browser are passed by the middleware. For example, in an embodiment where the systems interface 210 comprises protocol servers 240 and transaction servers 250 (FIG. 2), transaction servers 250 direct protocol servers 240 to route computer 200 from the first network address for protocol servers 240 to the separate network address for intranet 280. This routing permits computer 200 to leave the zone defined by firewall 260 for the systems interface and enter the zone defined by a firewall (not shown) for the intranet 280.

[0037] The firewall designates the allowable network destinations for incoming messages. The firewall has administrator-defined tables that lists acceptable destinations. Thus, specific locations or zones can be excluded. Intranet only access may be specified if the administrator so desires, and internet access can be excluded. The protocol server pass the incoming session along to the network address specified in the "header" of the incoming session. In this embodiment, transaction servers 250 send protocol servers 240 a message or command to effectuate this routing. Note that on incoming messages, transaction servers 250 are not involved if the incoming message requests a network address other than that of the transaction servers 250. Transaction servers 250 do not effectuate the routing, protocol servers 240 do. Only on outgoing messages that transaction servers 250 send header information to

protocol servers 240 (common user I.D.) that informs protocol servers 240 to whom the return message should be sent. According to an embodiment, the separate network address corresponds to a so-called "Technician Intranet Access Home Page."

[0038] According to a first embodiment, the Technician Intranet Access Home Page is a so-called "focused" web page on intranet 280. The user can view this focussed web page, which is updated on a regular basis by a web page administrator. The user may be able to submit queries from this web page. However, the user is not permitted to leave this web page to go to other sites in intranet 280.

[0039] In a second embodiment, the Technician Intranet Access Home Page is an introductory page that the user can leave to visit other sites on intranet 280. In this embodiment, the home page preferably includes links to other sites on the intranet that the user might wish to visit.

[0040] At this point, the technician using computer 200 has access to local information on intranet 280. The aforementioned client application (e.g., the TechNet client application) is still active and the user is still logged-in to systems interface 210 (e.g., TechNet system). Preferably, the client application is minimized or its window is hidden behind the browser window. For example, the TechNet home page may be hidden behind the Technician Intranet Access Home Page. Preferably, the user can toggle between the two applications (or windows) because both are active. The technician can return

to the systems interface (e.g., TechNet) by closing the browser or simply toggling between the two applications.

[0041] According to an embodiment, intranet 280 is a telephone company intranet serving various local offices of the telephone company. In this embodiment, the technician can access district-specific information such as cross-box locations, pricing information, service information, cable records, plat information, or other local information.

[0042] FIG. 3 is a flow diagram of a method for a user (e.g., a technician) to access an intranet according to an embodiment of the invention. FIG. 3 is explained below in connection with certain structure from the exemplary systems of FIG. 1 and FIG. 2. This is done in order to explain and illustrate the invention in a clear manner. However, the method is not limited or constrained by the structure of FIG. 1 or FIG. 2 or by any other structure.

[0043] In FIG. 3, a user, such as a technician, logs-on to the system (e.g., the TechNet system) in step 302. For example, a technician may log-on to a protocol server 240 of FIG. 2 by entering a user ID. The log-on may occur over a wireline network or over a wireless network.

[0044] In step 304, the technician's computer (e.g., computer 200 of FIG. 2) accesses the systems interface (e.g., element 130 of FIG. 1 or element 210 of FIG. 2) to back-end legacy systems (e.g., element 140 of FIG. 1 or element 270 of FIG. 2). According to an embodiment, the systems interface is accessed at a

first network address, preferably corresponding to a protocol server 240 (FIG. 2). The network address is preferrably an IP address.

[0045] In step 306, a shared network software application such as a browser is launched at the user's computer (e.g. computer 200 of FIG. 2).

[0046] In step 308, the user's computer accesses the intranet. In one embodiment, the user's computer accesses the intranet at a separate network address that is distinct from the aforementioned first network address. The separate network address is also preferably an IP address.

[0047] In step 310, an intranet home page is displayed. For example, a technician's computer 200 (FIG. 2) may display a Technician Intranet Home Page, previously discussed.

[0048] In step 312, the desired local information on the intranet (e.g., intranet 280 of FIG. 2) is retrieved. In one embodiment, a technician retrieves district-specific information such as cross-box locations, pricing information, service information, cable records, and plat information.

[0049] In step 314, the user returns to the systems interface to the legacy systems. For example, the user may toggle back to the TechNet client application or the user may close the browser application.

[0050] FIG. 4 is a flow diagram of a method for allowing a user (e.g., a technician) to access an intranet according to another embodiment of the invention. FIG. 4 is explained below in connection with certain structure from the exemplary systems of FIG. 1 and FIG. 2. This is done in order to clearly

explain the method, and it should not be construed that the method is limited or constrained by the structure of FIG. 1 or FIG. 2 or by any other structure.

[0051] In step 402, a log-in attempt by a user is authenticated. For example, a protocol server 240 (FIG. 2) may authenticate a technician attempting a log-in using computer 200 (FIG. 2). The log-in attempt may occur over a wireline network or over a wireless network.

[0052] In step 404, access to a systems interface to back-end legacy systems is provided. For example, computer 200 may be accessing protocol server 240 (FIG. 2) at a first network address.

[0053] In step 406, an attempt by the user to access an intranet is detected. For example, protocol server 240 (FIG. 2) may receive a message generated by computer 200 requesting intranet access. Protocol server 240 may detect that computer 200 is seeking a network address corresponding to intranet 280 (FIG. 2). Protocol server 240 could detect that the user is attempting to access the intranet in other fashions. The middleware in protocol server 240 hands off the TechNet transaction to the TechNet server. All other network addresses are sent to Intranet 280. Thus, if browser is started and nonTechNet network addresses is requested, protocol servers 240 hand that session off to Intranet 280.

[0054] It is noted that in one embodiment of the present invention, transaction server 250 can comprise two components. The first component, e.g., a Sun E-10000 system, performs a database administration function that authenticates

users according to data within the database that includes, for example, user ID, password, and PC serial number. The second component takes transaction requests from the user and, according to data in database, goes to the correct operations support system to effect the transaction. Protocol servers 240 pass the transaction on to the network address which is the header of the transaction.

[0055] In step 408, it is determined whether to grant access to the intranet. For example, transaction server 250 (FIG. 2) may determine whether a technician is logged-in to the TechNet system and/or whether that technician is permitted access to intranet 280 (FIG. 2). Access to the Intranet is provided by a firewall-access in or out of the protected zone is controlled by the firewall.

[0056] In step 410, the user is routed to the intranet. For example, communications from computer 200 (FIG. 2) may be routed from the first network address corresponding to the protocol server 240 (FIG. 2) to a separate network address corresponding to intranet 280 (FIG. 2). Preferably, the separate network address corresponds to a Technician Intranet home page, discussed above. In preferred embodiments, the network addresses are IP addresses.

[0057] The foregoing disclosure of the preferred embodiments of the present invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many variations and modifications of the embodiments described

herein will be obvious to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claims appended hereto, and by their equivalents.

[0058] Further, in describing representative embodiments of the present invention, the specification may have presented the method and/or process of the present invention as a particular sequence of steps. However, to the extent that the method or process does not rely on the particular order of steps set forth herein, the method or process should not be limited to the particular sequence of steps described. As one of ordinary skill in the art would appreciate, other sequences of steps may be possible. Therefore, the particular order of the steps set forth in the specification should not be construed as limitations on the claims. In addition, the claims directed to the method and/or process of the present invention should not be limited to the performance of their steps in the order written, and one skilled in the art can readily appreciate that the sequences may be varied and still remain within the spirit and scope of the present invention.